Smart Grid Interoperability Panel (SGIP)
Cyber Security Working Group (CSWG)
Standards Review

CSWG Standards Review Report on

Security Assessment of SAE J1772-3: SAE Electric Vehicle and Plug in Hybrid Electric Vehicle Conductive Charge Coupler

November 12, 2010

Security Assessment of SAE J1772-3: SAE Electric Vehicle and Plug in Hybrid Electric Vehicle Conductive Charge Coupler

1. Introduction

1.1 Correlation of Cybersecurity with Information Exchange Standards

Correlating cybersecurity with specific information exchange standards, including functional requirements standards, object modeling standards, and communication standards, is very complex. There is rarely a one-to-one correlation, with more often a one-to-many or many-to-one correspondence.

First, communication standards for the Smart Grid are designed to meet many different requirements at many different "layers" in the communications "stack" or "profile." One example of such a profile is the Grid Wise Architecture Council (GWAC)[1] Stack. Some standards address the lower layers of the communications stack, such as wireless media, fiber optic cables, and power line carrier. Others address the "transport" layers for getting messages from one location to another. Still others cover the "application" layers, the semantic structures of the information as it is transmitted between software applications. In addition, there are communication standards that are strictly abstract models of information – the relationships of pieces of information with each other. Since they are abstract, cybersecurity technologies cannot be linked to them until they are translated into "bits and bytes" by mapping them to one of the semantic structures. Above the communications standards are other security standards that address business processes and the policies of the organization and regulatory authorities.

Secondly, regardless of what communications standards are used, cybersecurity must address all layers – end-to-end – from the source of the data to the ultimate destination of the data. Cybersecurity must address those aspects outside of the communications system in the upper GWAC stack layers that may just be functional requirements or may rely on procedures rather than technologies, such as authenticating the users and software applications, and screening personnel. Cybersecurity must also address how to: cope during an attack, recover from it afterwards, and create a trail of forensic information to be used in post-attack analysis.

Thirdly, the cybersecurity requirements must reflect the environment where a standard is implemented rather than the standard itself: how and where a standard is used must establish the levels and types of cybersecurity needed. Communications standards do not address the importance of specific data or how it might be used in systems; these standards only address how to exchange the data. Standards related to the upper layers of the GWAC stack may address issues of data importance.

Fourthly, some standards do not mandate their provisions using "shall" statements, but rather use statements such as "should," "may," or "could." Some standards also define their provisions as being "normative" or "informative." Normative provisions often are expressed with "shall" statements. Various standards organizations use different terms (e.g., standard, guideline) to characterize their standards according to the kinds of statements used. If standards include security provisions, they need to be understood in the context of the "shall," "should," "may," and/or "could" statements, "normative," or "informative" language with which they are expressed.

Therefore, cybersecurity must be viewed as a stack or "profile" of different security technologies and procedures, woven together to meet the security requirements of a particular implementation of a stack of policy, procedural, and communication standards designed to provide specific services. Ultimately,

[1] GridWise Architecture Council, http://www.gridwiseac.org/pdfs/interopframework_v1.pdf

cybersecurity as applied to the information exchange standards should be described as profiles of technologies and procedures which can include both "power system" methods (e.g. redundant equipment, analysis of power system data, and validation of power system states) and information technology (IT) methods (e.g. encryption, role-based access control, and intrusion detection).

There also can be a relationship between certain communication standards and correlated cybersecurity technologies. For instance, if TCP/IP is being used at the transport layer and if authentication, data integrity, and/or confidentiality are important, then TLS (transport layer security) should most likely (but not absolutely) be used. For some specific Smart Grid communication standards, such as International Electrotechnical Commission (IEC) 61850 and IEC 60870-6, specific cybersecurity standards (IEC 62351 series) were developed to meet typical implementations of these standards.

In the following discussions of information exchange standard(s) being reviewed, these caveats should be taken into account.

1.2 Standardization Cycles of Information Exchange Standards

Information exchange standards, regardless of the standards organization, are developed over a time period of many months by experts who are trying to meet a specific need. In most cases, these experts are expected to revisit standards every five years in order to determine if updates are needed. In particular, since cybersecurity requirements were often not included in standards in the past, existing communication standards often have no references to security except in generalities, using language such as "appropriate security technologies and procedures should be implemented."

With the advent of the Smart Grid, cybersecurity has become increasingly important within the utility sector. However, since the development cycles of communication standards and cybersecurity standards are usually independent of each other, appropriate normative references between these two types of standards are often missing. Over time, these missing normative references can be added, as appropriate.

Since technologies (including cybersecurity technologies) are rapidly changing to meet increasing new and more powerful threats, some cybersecurity standards can be out-of-date by the time they are released. This means that some requirements in a security standard may be inadequate (due to new technology developments), while references to other security standards may be obsolete. This rapid improving of technologies and obsolescence of older technologies is impossible to avoid, but may be ameliorated by indicating minimum requirements and urging fuller compliance to new technologies as these are proven.

1.3 References and Terminology

References to the National Institute of Standards and Technology (NIST) security requirements refer to the NIST Interagency Report (IR) 7628, *Guidelines to Smart Grid Cyber Security*, Chapter 3, High-Level Security Requirements.

References to "government-approved cryptography" refer to the list of approved cryptography suites identified in Chapter 4, Cryptography and Key Management, of NISTIR 7628. Summary tables of the approved cryptography suites are provided in Chapter 4.3.2.1.

As noted, standards have different degrees for expressing requirements, and the security requirements must match these degrees. For these standards assessments, the following terminology is used to express these different degrees[2]:

[2] The first clause of each terminology definition comes from the International Electrotechnical Commission (IEC) Annex H of Part 2 of ISO/IEC Directives. The second clause (after "which") comes from the Institute of Electrical and Electronics Engineers (IEEE) as a further amplification of the term.

- Requirements are expressed by "…shall…," which indicates mandatory requirements strictly to be followed in order to conform to the standard and from which no deviation is permitted (*shall* equals *is required to*).
- Recommendations are expressed by "…should…," which indicates that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others; or that a certain course of action is preferred but not necessarily required (*should* equals *is recommended that*).
- Permitted or allowed items are expressed by "…may…," which is used to indicate a course of action permissible within the limits of the standard (*may* equals *is permitted to*).
- Ability to carry out an action is expressed by "…can …," which is used for statements of possibility and capability, whether material, physical, or causal (*can* equals *is able to*).
- The use of the word *must* is deprecated, and should not be used in these standards to define mandatory requirements. The word *must* is only used to describe unavoidable situations (e.g. "All traffic in this lane must turn right at the next intersection.")

2. SAE J1772-3: SAE Electric Vehicle and Plug in Hybrid Electric Vehicle Conductive Charge Coupler

2.1 Description of Standard

As stated in the Rationale and Foreword Sections, "*This recommended practice redefines AC Level 1 and AC Level 2 charge levels and specifies a new conductive charge coupler and electrical interfaces for AC Level 1 and AC Level 2 charging. The coupler and interfaces for DC charging are currently being developed and will be added to this document upon completion*."

"*Energy stored in a battery provides power for an Electric Vehicle (EV) or Plug In Hybrid Electric Vehicles (PHEV). Conductive charging is a method for connecting the electric power supply network to the EV/PHEV for the purpose of transferring energy to charge the battery and operate other vehicle electrical systems, establishing a reliable equipment grounding path, and exchanging control information between the EV/PHEV and the supply equipment. This document describes the electrical and physical interfaces between the EV/PHEV and supply equipment to facilitate conductive charging. Functional and performance requirements for the EV/PHEV and supply equipment are also specified*."

2.2 Assumptions and Issues

This document addresses the electrical and physical recommended practices for charging or discharging PEVs. It does not address any digital technology, and therefore does not address any cyber security.

2.3 Summary of Cybersecurity Content

2.3.1 Does the standard address cybersecurity? If not, should it?

This document does not address cybersecurity, but it does address physical safety concerns. There is no need to address cybersecurity..

2.3.2 What aspects of cybersecurity does the standard address and how well (correctly) does it do so?

This standard does not address any cybersecurity requirements as mapped to NISTIR 7628 high-level security requirements.

The correlations between this document and the security requirements described in NISTIR 7628, *Guidelines to Smart Grid Cybersecurity*, Chapter 3, families and requirements, are shown in Table 1:

Table 1: Correlations between Standard being Assessed and the NISTIR Security Requirements

Reference in Standard[3]	Applicable NISTIR 7628 Requirement	Comments if NISTIR Requirement Is Not Completely Met
None		

2.3.3 What aspects of cybersecurity does the standard not address? Which of these aspects should it address? Which should be handled by other means?

Because the standard only addresses electrical and physical requirements, no cybersecurity issues need to be addressed. However, the following issues should be considered in subsequent efforts:

- If PLC, wireless, or other potentially radiating technology is used for the communications, the traffic between the PEV and the EVSE should be encrypted. If no encryption, shielding, or other electromagnetic protection methods are used, there is a potential that confidential information (e.g., vehicle ID, credit card numbers, etc.) may be radiated in the clear between the EVSE and the PEV over power line carrier or wireless media.
- The normative and informative reference document list within SAE J1772-TM should be reviewed to determine if any cybersecurity requirements in those documents need to be updated or enhanced.

2.3.4 What work, if any, is being done currently or planned to address the gaps identified above? Is there a stated timeframe for completion of these planned modifications?

No known activity at this time, although it is expected that either a new PAP or DEWG will be formed.

2.3.5 List any references to other standards and whether they are normative or informative.

2.3.5.1 Normative References

- SAE J1113-21 Electromagnetic Compatibility Measurement Procedure for Vehicle Components—Part 21: Immunity to Electromagnetic Fields, 30 MHz to 18 GHz, Absorber-Lined Chamber
- SAE J1211 Handbook for Robustness Validation of Automotive Electrical/Electronic Modules
- SAE J1850 Class B Data Communications Network Interface

[3] The references may be just the section numbers or could include the title of the section

- SAE J2293-1 Energy Transfer System for Electric Vehicles—Part 1: Functional Requirements and System Architectures
- SAE J2293-2 Energy Transfer System for Electric Vehicles—Part 2: Communication Requirements and Network Architecture
- Canadian Electrical Code Part 1, Section 86
- CFR 40 Code of Federal Regulations—Title 40, Part 600, Subchapter Q
- CFR 47 Code of Federal Regulations—Title 47, Parts 15A, 15B, and 18C
- CISPR 12 Vehicles, boats and internal combustion engines—Radio disturbance characteristics—Limits and methods of measurement for the protection of off-board receivers
- 61000-4-6 Electromagnetic compatibility (EMC)—Part 4-6: Testing and measurement techniques—Immunity to conducted disturbances, induced by radiofrequency fields
- ISO 11451-2 Road vehicles—Vehicle test methods for electrical disturbances from narrowband radiated electromagnetic energy—Part 2: Off-vehicle radiation sources
- National Electrical Code, NFPA 70 Article 625 (2008 edition)
- UL 50 Standard for Enclosures for Electrical Equipment
- UL 1439 Determination of Sharpness of Edges on Equipment
- UL 2202 EV Charging System Equipment
- UL 2231-1 Personnel Protection Systems for Electric Vehicle Supply Circuits: General Requirements
- UL 2231-2 Personnel Protection Systems for Electric Vehicle Supply Circuits: Particular Requirements for Protection Devices for Use in Charging Systems
- UL 2251 Plugs, Receptacles, and Couplers for Electric Vehicles

2.3.5.2 Informative References

- SAE J551-5 Performance Levels and Methods of Measurement of Magnetic and Electric Field Strength from Electric Vehicles, Broadband, 9 kHz to 30 MHz
- SAE J1742 Connections for High Voltage On-Board Vehicle Electrical Wiring Harness—Test Methods and General Performance Requirements
- SAE J1773 SAE Electric Vehicle Inductively Coupled Charging
- SAE J1812 Function Performance Status Classification for EMC Immunity Testing
- SAE J2178-1 Class B Data Communication Network Messages—Detailed Header Formats and Physical Address Assignments
- SAE J2178-2 Class B Data Communication Network Messages—Part 2: Data Parameter Definitions
- SAE J2178-3 Class B Data Communication Network Messages—Part 3: Frame IDs for Single-Byte Forms of Headers
- SAE J2178-4 Class B Data Communication Network Messages—Message Definitions for Three Byte Headers

- 61000-4-3 Electromagnetic compatibility (EMC)—Part 4-3: Testing and measurement techniques—Radiated, radio-frequency, electromagnetic field immunity test
- IEC 61851-1 Electric Vehicle Conductive Charging System—Part 1: General Requirements
- IEC 61851-21 Electric Vehicle Conductive Charging System—Part 21: Electric Vehicle Requirements for Connection to an AC / DC Supply
- IEC 61851-22 Electric Vehicle Conductive Charging System—Part 22: AC Electric Vehicle Charging Station
- UL 94 Tests for Flammability of Plastic Materials for Parts in Devices and Appliances
- UL 231 Power Outlets
- UL 746A Standard for Polymeric Materials—Short Term Property Evaluations
- UL 840 Insulation Coordination Including Clearance and Creepage Distances for Electrical Equipment
- UL 2594 Outline of Investigation—Electric Vehicle Supply Equipment